


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
Search: The ACM Digital Library The Guide


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)
Terms used [file](#) [compar](#) [hash](#) [write access](#) [director](#)
Found 48 of 169,166
Sort results by

 [Save results to a Binder](#)
[Try an Advanced Search](#)
Display results

 [Search Tips](#)
[Try this search in The ACM Guide](#)
 [Open results in a new window](#)
Results 1 - 20 of 48
Result page: **1** [2](#) [3](#) [next](#)

Relevance scale

1 [General storage protection techniques: Securing distributed storage: challenges, techniques, and systems](#)

Vishal Kher, Yongdae Kim

 November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press

 Full text available: [pdf\(294.61 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

2 [Decentralized storage systems: Ivy: a read/write peer-to-peer file system](#)


Athicha Muthitacharoen, Robert Morris, Thamer M. Gil, Benjie Chen

 December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI

Publisher: ACM Press

 Full text available: [pdf\(1.65 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Ivy is a multi-user read/write peer-to-peer file system. Ivy has no centralized or dedicated components, and it provides useful integrity properties without requiring users to fully trust either the underlying peer-to-peer storage system or the other users of the file system. An Ivy file system consists solely of a set of logs, one log per participant. Ivy stores its logs in the DHash distributed hash table. Each participant finds data by consulting all logs, but performs modifications by appendi ...

3 [Dynamic Metadata Management for Petabyte-Scale File Systems](#)

Sage A. Weil, Kristal T. Pollack, Scott A. Brandt, Ethan L. Miller

 November 2004 **Proceedings of the 2004 ACM/IEEE conference on Supercomputing**
Publisher: IEEE Computer Society

 Full text available: [pdf\(175.04 KB\)](#) Additional Information: [full citation](#), [abstract](#)

In petabyte-scale distributed file systems that decouple read and write from metadata

operations, behavior of the metadata server cluster will be critical to overall system performance and scalability. We present a dynamic subtree partitioning and adaptive metadata management system designed to efficiently manage hierarchical metadata workloads that evolve over time. We examine the relative merits of our approach in the context of traditional workload partitioning strategies, and demonstrate the ...

4 The Vesta parallel file system

 Peter F. Corbett, Dror G. Feitelson

August 1996 **ACM Transactions on Computer Systems (TOCS)**, Volume 14 Issue 3

Publisher: ACM Press

Full text available:  [pdf\(649.08 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

The Vesta parallel file system is designed to provide parallel file access to application programs running on multicomputers with parallel I/O subsystems. Vesta uses a new abstraction of files: a file is not a sequence of bytes, but rather it can be partitioned into multiple disjoint sequences that are accessed in parallel. The partitioning—which can also be changed dynamically—reduces the need for synchronization and coordination during the access. Some control over the layout ...

Keywords: data partitioning, parallel computing, parallel file system

5 Services: ELF: an efficient log-structured flash file system for micro sensor nodes

 Hui Dai, Michael Neufeld, Richard Han

November 2004 **Proceedings of the 2nd international conference on Embedded networked sensor systems**

Publisher: ACM Press

Full text available:  [pdf\(291.68 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

An efficient and reliable file storage system is important to micro sensor nodes so that data can be logged for later asynchronous delivery across a multi-hop wireless sensor network. Designing and implementing such a file system for a sensor node faces various challenges. Sensor nodes are highly resource constrained in terms of limited runtime memory, limited persistent storage, and finite energy. Also, the flash storage medium on sensor nodes differs in a variety of ways from the traditional ...

Keywords: eeprom, file system, flash, log structured, reliability, sensor

6 The Alpine file system

 M. R. Brown, K. N. Kolling, E. A. Taft

November 1985 **ACM Transactions on Computer Systems (TOCS)**, Volume 3 Issue 4

Publisher: ACM Press

Full text available:  [pdf\(2.95 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Alpine is a file system that supports atomic transactions and is designed to operate as a service on a computer network. Alpine's primary purpose is to store files that represent databases. An important secondary goal is to store ordinary files representing documents, program modules, and the like. Unlike other file servers described in the literature, Alpine uses a log-based technique to implement atomic file update. Another unusual aspect of Alpine is that it performs all commu ...

7

Access Control Models and Mechanisms: Cryptographic access control in a distributed file system

Anthony Harrington, Christian Jensen
 June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies**

Publisher: ACM Press

Full text available:  [pdf\(249.24 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Traditional access control mechanisms rely on a reference monitor to mediate access to protected resources. Reference monitors are inherently centralized and existing attempts to distribute the functionality of the reference monitor suffer from problems of scalability. Cryptographic access control is a new distributed access control paradigm designed for a global federation of information systems. It defines an implicit access control mechanism, which relies exclusively on cryptography to provide ...

Keywords: access control, cryptography, network file systems

8 **Decentralized storage systems: Farsite: federated, available, and reliable storage for an incompletely trusted environment**

Atul Adya, William J. Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R. Douceur, Jon Howell, Jacob R. Lorch, Marvin Theimer, Roger P. Wattenhofer
 December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI

Publisher: ACM Press

Full text available:  [pdf\(1.87 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Farsite is a secure, scalable file system that logically functions as a centralized file server but is physically distributed among a set of untrusted computers. Farsite provides file availability and reliability through randomized replicated storage; it ensures the secrecy of file contents with cryptographic techniques; it maintains the integrity of file and directory data with a Byzantine-fault-tolerant protocol; it is designed to be scalable by using a distributed hint mechanism and delegatio ...

9 **801 storage: architecture and programming**

Albert Chang, Mark F. Mergen
 February 1988 **ACM Transactions on Computer Systems (TOCS)**, Volume 6 Issue 1

Publisher: ACM Press

Full text available:  [pdf\(1.87 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Based on novel architecture, the 801 minicomputer project has developed a low-level storage manager that can significantly simplify storage programming in subsystems and applications. The storage manager embodies three ideas: (1) large virtual storage, to contain all temporary data and permanent files for the active programs; (2) the innovation of database storage, which has implicit properties of access serializability and atomic update, similar to those o ...

10 **FS2: dynamic data replication in free disk space for improving disk performance and energy consumption**

Hai Huang, Wanda Hung, Kang G. Shin
 October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available:  [pdf\(542.63 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Disk performance is increasingly limited by its head positioning latencies, i.e., seek time and rotational delay. To reduce the head positioning latencies, we propose a novel technique that *dynamically* places copies of data in file system's *free blocks* according to

the disk access patterns observed at runtime. As one or more replicas can now be accessed in addition to their original data block, choosing the "nearest" replica that provides fastest access can significantly improve pe ...

Keywords: data replication, disk layout reorganization, dynamic file system, free disk space

11 The architecture of robust publishing systems

 Marc Waldman, Aviel D. Rubin, Lorrie Faith Cranor

November 2001 **ACM Transactions on Internet Technology (TOIT)**, Volume 1 Issue 2

Publisher: ACM Press

Full text available:  [pdf\(680.21 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The Internet in its present form does not protect content from censorship. It is straightforward to trace any document back to a specific Web server, and usually directly to an individual. As we discuss below, there are valid reasons for publishing a document in a censorship-resistant manner. Unfortunately, few tools exist that facilitate this form of publishing. We describe the architecture of robust systems for publishing content on the Web. The discussion is in the context of Publius, as that ...

Keywords: Censorship resistance, Web publishing

12 PARADISE: an advanced featured parallel file system

 Maciej Brodowicz, Olin Johnson

July 1998 **Proceedings of the 12th international conference on Supercomputing**

Publisher: ACM Press

Full text available:  [pdf\(992.07 KB\)](#) Additional Information: [full citation](#), [references](#), [index terms](#)

13 Affinity-based management of main memory database clusters

 Minwen Ji

November 2002 **ACM Transactions on Internet Technology (TOIT)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available:  [pdf\(553.96 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We study management strategies for main memory database clusters that are interposed between Internet applications and back-end databases as content caches. The task of management is to allocate data across individual cache databases and to route queries to the appropriate databases for execution. The goal is to maximize effective cache capacity and to minimize synchronization cost. We propose an affinity-based management system for main memory database cLusters (ALBUM). ALBUM executes ea ...

Keywords: Main memory database, clustering, database administration, database cluster, file organization, query affinity, scalability

14 HFS: a performance-oriented flexible file system based on building-block

 compositions

Orran Krieger, Michael Stumm

August 1997 **ACM Transactions on Computer Systems (TOCS)**, Volume 15 Issue 3

Publisher: ACM Press

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

Full text available: [pdf\(383.87 KB\)](#)[terms, review](#)

The Hurricane File System (HFS) is designed for (potentially large-scale) shared-memory multiprocessors. Its architecture is based on the principle that, in order to maximize performance for applications with diverse requirements, a file system must support a wide variety of file structures, file system policies, and I/O interfaces. Files in HFS are implemented using simple building blocks composed in potentially complex ways. This approach yields great flexibility, allowing an application ...

Keywords: customization, data partitioning, data replication, flexibility, parallel computing, parallel file system

15 RAID: high-performance, reliable secondary storage

 Peter M. Chen, Edward K. Lee, Garth A. Gibson, Randy H. Katz, David A. Patterson
June 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 2

Publisher: ACM Press

Full text available: [pdf\(3.60 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Disk arrays were proposed in the 1980s as a way to use parallelism between multiple disks to improve aggregate I/O performance. Today they appear in the product lines of most major computer manufacturers. This article gives a comprehensive overview of disk arrays and provides a framework in which to organize current and future work. First, the article introduces disk technology and reviews the driving forces that have popularized disk arrays: performance and reliability. It discusses the tw ...

Keywords: RAID, disk array, parallel I/O, redundancy, storage, striping

16 Safely executing untrusted code: Model-carrying code: a practical approach for safe execution of untrusted applications

 R. Sekar, V.N. Venkatakrishnan, Samik Basu, Sandeep Bhatkar, Daniel C. DuVarney
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Publisher: ACM Press

Full text available: [pdf\(301.30 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper presents a new approach called *model-carrying code* (MCC) for safe execution of untrusted code. At the heart of MCC is the idea that untrusted code comes equipped with a concise high-level model of its security-relevant behavior. This model helps bridge the gap between high-level security policies and low-level binary code, thereby enabling analyses which would otherwise be impractical. For instance, users can use a fully automated verification procedure to determine if the code ...

Keywords: mobile code security, policy enforcement, sand-boxing, security policies

17 Hive: fault containment for shared-memory multiprocessors

 J. Chapin, M. Rosenblum, S. Devine, T. Lahiri, D. Teodosiu, A. Gupta
December 1995 **ACM SIGOPS Operating Systems Review, Proceedings of the fifteenth ACM symposium on Operating systems principles SOSP '95**, Volume 29 Issue 5

Publisher: ACM Press

Full text available: [pdf\(1.90 MB\)](#)Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

18 Operating System Structures to Support Security and Reliable Software Theodore A. LindenDecember 1976 **ACM Computing Surveys (CSUR)**, Volume 8 Issue 4

Publisher: ACM Press

Full text available:  pdf(3.49 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)**19 Astrolabe: A robust and scalable technology for distributed system monitoring,** management, and data mining

Robbert Van Renesse, Kenneth P. Birman, Werner Vogels

May 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 2

Publisher: ACM Press

Full text available:  pdf(341.62 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Scalable management and self-organizational capabilities are emerging as central requirements for a generation of large-scale, highly dynamic, distributed applications. We have developed an entirely new distributed information management system called Astrolabe. Astrolabe collects large-scale system state, permitting rapid updates and providing on-the-fly attribute aggregation. This latter capability permits an application to locate a resource, and also offers a scalable way to track sys ...

Keywords: Aggregation, epidemic protocols, failure detection, gossip, membership, publish-subscribe, scalability

20 Configuration management & security: Secure sharing between untrusted users in a transparent source/binary deployment model

Eelco Dolstra

November 2005 **Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering ASE '05**

Publisher: ACM Press

Full text available:  pdf(276.98 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The Nix software deployment system is based on the paradigm of *transparent source/binary deployment*: distributors deploy descriptors that build components from source, while client machines can transparently optimise such source builds by downloading pre-built binaries from remote repositories. This model combines the simplicity and flexibility of source deployment with the efficiency of binary deployment. A desirable property is *sharing* of components: if multiple users install fro ...

Keywords: configuration management, hash rewriting, secure sharing, security, software deployment, source deployment

Results 1 - 20 of 48

Result page: [1](#) [2](#) [3](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)

Set	Items	Description
S1	92909	(AUTHORI?????? OR PERMIT???? OR PERMISSION? ? OR ALLOW???) - (3N) (ACCESS??? OR WRIT??? OR READ??? OR MODIFY??? OR MODIFI?? - ????? OR CHANG???)
S2	11800849	FILE? ? OR FILENAME? ? OR INFORMATION OR DATA
S3	179404	(FIRST OR 1ST OR ONE) (3N) S2
S4	401160	(TWO OR SECOND OR 2ND OR NEXT OR ANOTHER OR OTHER) (3N) S2
S5	379114	(COMPAR??? OR COMPARISON? ? OR MATCH???) (3N) S2
S6	12665	(HASH??? OR ENCRYPT???) (3N) S2
S7	36908	(TWO OR SECOND OR 2ND OR NEXT OR ANOTHER OR OTHER) (3N) KEY? ?
S8	479	(COMBIN????? OR CONCATENAT??? OR CONJOIN??? OR JOIN??? OR - TOGETHER OR MERG??? OR COMPOUND???) (3N) S7
S9	426	S5(5N) S3(5N) S4
S10	1	S1 AND S9
S11	3	S1 AND S3 AND S4 AND S5
S12	2	S11 NOT S10
S13	57	S1(5N) S5
S14	38	RD (unique items)
S15	0	S14 AND S6
S16	33	S14 NOT PY=2002:2006
S17	33	S16 NOT (S10 OR S12)
S18	369319	FILE? ? OR FILENAME? ?
S19	6487	(FIRST OR 1ST OR ONE) (3N) S18
S20	10396	(TWO OR SECOND OR 2ND OR NEXT OR ANOTHER OR OTHER) (3N) S18
S21	2370	(COMPAR??? OR COMPARISON? ? OR MATCH???) (3N) S18
S22	27	S19(10N) S20(10N) S21
S23	0	S22 AND S1
S24	165	(S19 OR S20) (5N) S21
S25	1	S24 AND S1
S26	24	S22 NOT PY=2002:2006
S27	15	RD (unique items)
S28	15	S27 NOT (S10 OR S12 OR S17)
S29	51479	(AUTHORI?????? OR PERMIT???? OR PERMISSION? ? OR ALLOW???) - (3N) (WRITE OR WRITING OR MODIF? OR CHANG???)
S30	0	S29(10N) S21
S31	2	S29 AND S21
S32	892	(COMPAR??? OR COMPARISON? ? OR MATCH???) (3N) (HASH??? OR EN- CRYPT???)
S33	3	S29(10N) S32
S34	3	S29 AND S32
S35	1	S8 AND S1
S36	27	S8 AND (CRYPTO? OR ENCRYPT?)
S37	16	RD (unique items)
S38	8	S37 NOT PY=2002:2006
File	2:INSPEC 1898-2006/Dec W3	
		(c) 2006 Institution of Electrical Engineers
File	6:NTIS 1964-2006/Jan W1	
		(c) 2006 NTIS, Intl Cpyrght All Rights Res
File	8:Ei Compendex(R) 1970-2006/Jan W1	
		(c) 2006 Elsevier Eng. Info. Inc.
File	23:CSA Technology Research Database 1963-2005/Dec	
		(c) 2005 CSA.
File	34:SciSearch(R) Cited Ref Sci 1990-2006/Jan W1	
		(c) 2006 Inst for Sci Info
File	35:Dissertation Abs Online 1861-2005/Dec	
		(c) 2005 ProQuest Info&Learning
File	65:Inside Conferences 1993-2006/Jan W2	
		(c) 2006 BLDSC all rts. reserv.
File	94:JICST-Eplus 1985-2006/Oct W5	
		(c) 2006 Japan Science and Tech Corp(JST)

File 99:Wilson Appl. Sci & Tech Abs 1983-2006/Dec
(c) 2006 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Jan 09
(c) 2006 The Gale Group
File 144:Pascal 1973-2006/Dec W3
(c) 2006 INIST/CNRS
File 239:Mathsci 1940-2005/Feb
(c) 2005 American Mathematical Society
File 256:TecInfoSource 82-2005/Feb
(c) 2005 Info.Sources Inc
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group
File 474:New York Times Abs 1969-2006/Jan 11
(c) 2006 The New York Times
File 475:Wall Street Journal Abs 1973-2006/Jan 11
(c) 2006 The New York Times

38/5/5 (Item 5 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2006 Institution of Electrical Engineers. All rts. reserv.

03493286 INSPEC Abstract Number: C85038249

Title: Employing one-way function methods for PIN verification and composite key generation in electronic funds transfer systems

Author(s): Holloway, C.J.; Meyer, C.H.

Author Affiliation: IBM UK Ltd., London, UK

Conference Title: International Data Security Conference 1985 p.17 pp.

Publisher: Open Comput. Security, Brighton, UK

Publication Date: 1985 Country of Publication: UK 210 pp.

Conference Date: 18-19 Feb. 1985 Conference Location: London, UK

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: One essential requirement of an electronic fund transfer (EFT) system is that institutions must be able to join together in a common EFT network, defined as an interchange, such that the EFT security of each institution is independent of the security measures implemented at other institutions. It is demonstrated how to achieve this by employing one-way function methods for personal identification number (PIN) verification, as well as for establishing end-to-end **cryptographic** keys. In the PIN verification approach, issuer based validation schemes are discussed which allow personal verification at either the terminal or at the issuer with equal security. The one-way function approach provides the designer therefore with another option and increases his flexibility to achieve business objectives. Two different end-to-end key management techniques are described and analyzed. The first one uses an end-to-end system key which can also be **combined** with a personal **key**. The **second** one generates an end-to-end key based on a node key component and a personal key. It is shown that, although the first approach is theoretically more secure, the second option offers implementation advantages in complex networks at entirely adequate security levels. (5 Refs)

Subfile: C

Descriptors: EFTS; security of data

Identifiers: one-way function methods; PIN verification; composite key generation; electronic funds transfer systems; EFT network; interchange; security measures; personal identification number; end-to-end **cryptographic** keys; issuer based validation schemes; personal verification; node key component; personal key; implementation; complex networks

Class Codes: C0310D (Installation management); C6130 (Data handling techniques); C7120 (Finance)

Set	Items	Description
S1	61260	(AUTHORI?????? OR PERMIT???? OR PERMISSION? ? OR ALLOW???) - (3N) (ACCESS??? OR WRIT??? OR READ??? OR MODIFY??? OR MODIFI?? - ????? OR CHANG???)
S2	3088425	FILE? ? OR FILENAME? ? OR INFORMATION OR DATA
S3	159516	(FIRST OR 1ST OR ONE) (3N) S2
S4	218131	(TWO OR SECOND OR 2ND OR NEXT OR ANOTHER OR OTHER) (3N) S2
S5	85458	(COMPAR??? OR COMPARISON? ? OR MATCH???) (3N) S2
S6	11033	(HASH??? OR ENCRYPT???) (3N) S2
S7	16171	(TWO OR SECOND OR 2ND OR NEXT OR ANOTHER OR OTHER) (3N) KEY? ?
S8	361	(COMBIN????? OR CONCATENAT??? OR CONJOIN??? OR JOIN??? OR - TOGETHER OR MERG??? OR COMPOUND???) (3N) S7
S9	0	S1 AND S3 AND S4 AND S5 AND S6 AND S7 AND S8
S10	1467	S5(5N)S3(5N)S4
S11	12	S1 AND S10
S12	8	S11 NOT AD=20011005:20031005/PR
S13	8	S12 NOT AD=20031005:20060111/PR
S14	7	S5(10N)S6 AND S1
S15	7	S14 NOT S13
S16	4	S15 NOT AD=20011005:20031005/PR
S17	4	S16 NOT AD=20031005:20060111/PR
S18	648	(COMPAR??? OR COMPARISON? ? OR MATCH???) (3N) (HASH??? OR EN- CRYPT???)
S19	19	S18 AND S1
S20	18	S19 NOT (S13 OR S17)
S21	18	S20 AND IC=(H04L OR G06F)
S22	13	S21 NOT AD=20011005:20031005/PR
S23	11	S22 NOT AD=20031005:20060111/PR
S24	7	S8 AND S1
S25	7	S24 NOT (S13 OR S17 OR S11)
File 347:JAPIO Nov 1976-2005/Aug (Updated 051205) (c) 2005 JPO & JAPIO		
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200602 (c) 2006 Thomson Derwent		

Set	Items	Description
S1	133506	(AUTHORI?????? OR PERMIT???? OR PERMISSION? ? OR ALLOW???) - (3N) (ACCESS??? OR WRIT??? OR READ??? OR MODIFY??? OR MODIFI?? - ????? OR CHANG???)
S2	1457133	FILE? ? OR FILENAME? ? OR INFORMATION OR DATA
S3	220174	(FIRST OR 1ST OR ONE) (3N) S2
S4	260468	(TWO OR SECOND OR 2ND OR NEXT OR ANOTHER OR OTHER) (3N) S2
S5	78991	(COMPAR??? OR COMPARISON? ? OR MATCH???) (3N) S2
S6	19336	(HASH??? OR ENCRYPT???) (3N) S2
S7	33803	(TWO OR SECOND OR 2ND OR NEXT OR ANOTHER OR OTHER) (3N) KEY? ?
S8	1255	(COMBIN????? OR CONCATENAT??? OR CONJOIN??? OR JOIN??? OR - TOGETHER OR MERG??? OR COMPOUND???) (3N) S7
S9	2824	S5(5N) S3(5N) S4
S10	63	S9(S) S1
S11	12	S10(S) S6
S12	9	S11 NOT AD=20011005:20031005/PR
S13	6	S12 NOT AD=20031005:20060111/PR
S14	57	S10 NOT S13
S15	36	S14 AND IC=(H04L OR G06F)
S16	24	S15 NOT AD=20011005:20031005/PR
S17	21	S16 NOT AD=20031005:20060111/PR
S18	540	S5(3N) S6
S19	56453	(AUTHORI?????? OR PERMIT???? OR PERMISSION? ? OR ALLOW???) - (3N) (WRIT??? OR MODIFY??? OR MODIFI?????? OR CHANG???)
S20	12	S19(10N) S18
S21	12	S20 NOT (S13 OR S17)
S22	10	S21 NOT AD=20011005:20031005/PR
S23	10	S22 NOT AD=20031005:20060111/PR
S24	42	S8(S) S1
S25	23	S24 AND IC=(H04L OR G06F)
S26	22	S25 NOT (S13 OR S17 OR S21)
S27	15	S26 NOT AD=20011005:20031005/PR
S28	14	S27 NOT AD=20031005:20060111/PR

File 348:EUROPEAN PATENTS 1978-2005/Dec W04

(c) 2005 European Patent Office

File 349:PCT FULLTEXT 1979-2005/UB=20051229,UT=20051222

(c) 2005 WIPO/Univentio

28/3,K/5 (Item 5 from file: 348)

DIALOG(R) File 348:EUROPEAN PATENTS

(c) 2005 European Patent Office. All rts. reserv.

00602380

Cryptography system
Verschlüsselungseinrichtung
Système cryptographique

PATENT ASSIGNEE:

International Business Machines Corporation, (200120), Old Orchard Road,
Armonk, N.Y. 10504, (US), (Proprietor designated states: all)

INVENTOR:

Merrick, Roland Albert, 8 St James Close, Harvington, Nr Evesham,
Worcestershire WR11 5PZ, (GB)

LEGAL REPRESENTATIVE:

Burt, Roger James, Dr. (52152), IBM United Kingdom Limited Intellectual
Property Department Hursley Park, Winchester Hampshire SO21 2JN, (GB)

PATENT (CC, No, Kind, Date): EP 604008 A1 940629 (Basic)

EP 604008 B1 010523

APPLICATION (CC, No, Date): EP 93308761 931102;

PRIORITY (CC, No, Date): GB 9226511 921219

DESIGNATED STATES: DE; FR; GB

INTERNATIONAL PATENT CLASS: G06F-012/14 ; H04L-009/08

ABSTRACT WORD COUNT: 143

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200121	553
CLAIMS B	(German)	200121	642
CLAIMS B	(French)	200121	682
SPEC B	(English)	200121	3238
Total word count - document A			0
Total word count - document B			5115
Total word count - documents A + B			5115

INTERNATIONAL PATENT CLASS: G06F-012/140 ...

... H04L-009/08

...SPECIFICATION length key. In a preferred embodiment, the second keys are stored in encrypted form, and **access** restricted to **authorised** users. It may also be possible to **combine** the first and **second keys** in some relatively sophisticated way to generate the full-length key, rather than simply append...

17/3,K/5 (Item 5 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
(c) 2005 European Patent Office. All rts. reserv.

00965408

METHOD AND SYSTEM FOR IMPROVING SECURITY IN NETWORK APPLICATIONS
VERFAHREN UND EINRICHTUNG ZUR VERBESSERUNG DER SICHERHEIT IN
NETZWERKANWENDUNGEN
PROCEDE ET SYSTEME D'AMELIORATION DE LA SECURITE DANS DES APPLICATIONS DE
RESEAU

PATENT ASSIGNEE:

ACTIVCARD IRELAND LIMITED, (4032120), 30 Herbert Street, Dublin 2, (IE),
(Proprietor designated states: all)

INVENTOR:

BORZA, Stephen, J., 495 Metcalfe Street, Ottawa, Ontario K1S 3N3, (CA)

LEGAL REPRESENTATIVE:

Colas, Jean-Pierre et al (14814), Cabinet JP Colas 37, avenue Franklin D.
Roosevelt, 75008 Paris, (FR)

PATENT (CC, No, Kind, Date): EP 944980 A1 990929 (Basic)
EP 944980 B1 030326
WO 98025385 980611

APPLICATION (CC, No, Date): EP 97946968 971202; WO 97CA926 971202

PRIORITY (CC, No, Date): US 32347 P 961204; US 907958 970811

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU;
MC; NL; PT; SE

INTERNATIONAL PATENT CLASS: H04L-029/06 ; G06F-001/00

NOTE:

No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200313	2196
CLAIMS B	(German)	200313	2287
CLAIMS B	(French)	200313	2329
SPEC B	(English)	200313	9908
Total word count - document A			0
Total word count - document B			16720
Total word count - documents A + B			16720

INTERNATIONAL PATENT CLASS: H04L-029/06 ...

... G06F-001/00

...SPECIFICATION computer to produce data using the process for
characterising user authorisation information;

(d) transmitting the data to the **first** computer; and

(e) **comparing** the data received by the **first** computer to

information on the **first** computer to determine a value and when the
value is within predetermined limits performing one of identifying a
source of the biometric information and **authorising** access from the
second other computer to information secured by the **first** computer.

Brief Description of...

28/3,K/4 (Item 4 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
(c) 2005 European Patent Office. All rts. reserv.

00662297

Method of software distribution protection

Software-Verteilungsschutzverfahren

Methode de protection de distribution de logiciels

PATENT ASSIGNEE:

SOFTWARE SECURITY, INC., (1409330), 1011 High Ridge Road, Stamford, CT 06905, (US), (Proprietor designated states: all)

INVENTOR:

Chou, Wayne, W., 25 Hauley Place, Ridgefield, Connecticut 06877, (US)
Kulinets, Joseph M., 40 Meredith Lane, Stamford, Connecticut 06903, (US)
Elteto, Laszlo, 86 Snow Crystal Lane, Stamford, Connecticut 06905, (US)
Engel, Frederick, 203 Middlebrook Farm Road, Wilton, Connecticut 06897, (US)

LEGAL REPRESENTATIVE:

Wachtershauser, Gunter, Prof. Dr. (12711), Patentanwalt, Tal 29, 80331 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 636962 A2 950201 (Basic)

EP 636962 A3 990217

EP 636962 B1 030827

APPLICATION (CC, No, Date): EP 94109291 940616;

PRIORITY (CC, No, Date): US 97705 930727

DESIGNATED STATES: DE; FR; GB

INTERNATIONAL PATENT CLASS: G06F-001/00 ; G06F-012/14

ABSTRACT WORD COUNT: 120

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	468
CLAIMS B	(English)	200335	260
CLAIMS B	(German)	200335	276
CLAIMS B	(French)	200335	290
SPEC A	(English)	EPABF2	1901
SPEC B	(English)	200335	1986
Total word count - document A			2369
Total word count - document B			2812
Total word count - documents A + B			5181

INTERNATIONAL PATENT CLASS: G06F-001/00 ...

... G06F-012/14

...SPECIFICATION of the file requested, to a processing center. It is checked whether the user is **authorized** to **access** the file, based on credit conditions and user identification. If the user is authorized, a ...

...key that is unique to the user. This information is read and checked, and the **two keys** are **combined** in an algorithm for generating a decryption key for decrypting the distributed file.

US patent...

17/3,K/6 (Item 1 from file: 349)
DIALOG(R) File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00943767 **Image available**

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR A SUPPLY CHAIN MANAGEMENT
Système, Procédé et Produit Programme Informatique Concus Pour Une Gestion
de Chaîne d'approvisionnement

Patent Applicant/Assignee:

RESTAURANT SERVICES INC, Two Alhambra Plaza, Suite 500, Coral Gables, FL
33134-5202, US, US (Residence), US (Nationality), (For all designated
states except: US)

Patent Applicant/Inventor:

HOFFMANN George Harry, Restaurant Services, Inc., Two Alhambra Plaza,
Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US
(Nationality), (Designated only for: US)

BURK Michael James, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

MENNINGER Anthony Frank, Restaurant Services, Inc., Two Alhambra Plaza,
Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US
(Nationality), (Designated only for: US)

GREENE Edward Arthur, Restaurant Services, Inc., Two Alhambra Plaza,
Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US
(Nationality), (Designated only for: US)

SMITH Mark Alan, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

TOMAS-FLYNN Martha Helen, Restaurant Services, Inc., Two Alhambra Plaza,
Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US
(Nationality), (Designated only for: US)

REECE Debra Gayle, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

SECHRIST Daniel, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

EKEY Diane Karen, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

RUEFF Mark Patrick, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

BARNETT John B, Restaurant Services, Inc., Two Alhambra Plaza, Suite 500,
Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

RODRIGUEZ Wendy, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

MARKS Stephen Patrick, Restaurant Services, Inc., Two Alhambra Plaza,
Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US
(Nationality), (Designated only for: US)

FOURAKER William Vance, Restaurant Services, Inc., Two Alhambra Plaza,
Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US
(Nationality), (Designated only for: US)

HYATT James F II, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

DIAZ Adriana Maria, Restaurant Services, Inc., Two Alhambra Plaza, Suite
500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality),
(Designated only for: US)

KIRSHENBAUM Laurence Joseph, Restaurant Services, Inc., Two Alhambra Plaza, Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality), (Designated only for: US)
BESSETTE Robert John, Restaurant Services, Inc., Two Alhambra Plaza, Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality), (Designated only for: US)
GEHMAN Anson Jerome, Restaurant Services, Inc., Two Alhambra Plaza, Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality), (Designated only for: US)
MOR Richardo, Restaurant Services, Inc., Two Alhambra Plaza, Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality), (Designated only for: US)
BURNS Michael Paul, Restaurant Services, Inc., Two Alhambra Plaza, Suite 500, Coral Gables, FL 33134-5202, US, US (Residence), US (Nationality), (Designated only for: US)

Legal Representative:

ELLIS William T (et al) (agent), Foley & Lardner, Washington Harbour, 3000 K Street, N.W., Suite 500, Washington, D.C. 20007-5109, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200277917 A1 20021003 (WO 0277917)
Application: WO 2002US8287 20020319 (PCT/WO US02008287)
Priority Application: US 2001816567 20010322; US 2001815598 20010323; US 2001816565 20010323; US 2001816488 20010323; US 2001816426 20010323; US 2001815899 20010323; US 2001816507 20010323; US 2001816422 20010323; US 2001816269 20010323; US 2001816491 20010323; US 2001816101 20010323; US 2001816231 20010323; US 2001816421 20010323; US 2001816069 20010323; US 2001816296 20010323; US 2001816249 20010323; US 2001816121 20010323; US 2001815668 20010323; US 2001816187 20010323; US 2001815490 20010323; US 2001816471 20010323; US 2001815606 20010323; US 2001815777 20010323; US 2001815813 20010323; US 2001816429 20010323; US 2001815515 20010323; US 2001816543 20010323; US 2001816349 20010323; US 2001816331 20010323; US 2001816167 20010323; US 2001816881 20010323; US 2001816536 20010323; US 2001816092 20010323; US 2001816576 20010323; US 2001815759 20010323; US 2001816495 20010323; US 2001816976 20010323; US 2001816083 20010323; US 2001815715 20010323; US 2001815989 20010323; US 2001816561 20010323; US 2001815483 20010323; US 2001816553 20010323; US 2001815688 20010323; US 2001816388 20010323; US 2001816358 20010323; US 2001815729 20010323; US 2001816537 20010323; US 2001816434 20010323; US 2001815897 20010323; US 2001815734 20010323; US 2001816431 20010323; US 2001816021 20010323; US 2001816454 20010323; US 2001816413 20010323; US 2001816430 20010323; US 2001816428 20010323; US 2001815830 20010323; US 2001816922 20010323; US 2001815489 20010323; US 2001816048 20010323; US 2001815727 20010323; US 2001816212 20010323; US 2001815660 20010323; US 2001815894 20010323; US 2001816151 20010323; US 2001816582 20010323; US 2001816033 20010323; US 2001816357 20010323; US 2001816420 20010323; US 2001815731 20010323; US 2001816503 20010323; US 2001816160 20010323; US 2001815893 20010323; US 2001816414 20010323; US 2001815792 20010323; US 2001815864 20010323; US 2001816896 20010323; US 2001815725 20010323; US 2001816285 20010323; US 2001815973 20010323; US 2001815845 20010323; US 2001816314 20010323; US 2001816075 20010323; US 2001816944 20010323; US 2001815559 20010323; US 2001816203 20010323; US 2001816567 20010323; US 2001816268 20010323; US 2001816424 20010323; US 2001816564 20010323; US 2001816455 20010323; US 2001816412 20010323; US 2001815590 20010323; US 2001816555 20010323; US 2001816560 20010323; US 2001816427 20010323; US 2001834600 20010413; US 2001834838 20010413; US 2001834924 20010413; US 2001834465 20010413

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI

SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 114107

...International Patent Class: G06F-017/60

Fulltext Availability:

Claims

Claim

... the network, the data relating to the sale of goods by the stores and including **second** identification **information** more recent than the **first** identification **information** ;
C) **allowing access** to the data utilizing a network-based interface;
d) **comparing** the **first** identification **information** with the **second** identification **information** ; and
e) updating the registration of the stores based on the comparison. 104.
A system...

...and including second identification information more recent than the first identification information; C) logic for **allowing access** to the data utilizing a network-based interface; d) logic for **comparing** the **first** identification **information** with the **second** identification **information** ; and
e) logic for updating the registration of the stores based on the comparison. 105...

23/5/1 (Item 1 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2006 Thomson Derwent. All rts. reserv.

014929398 **Image available**

WPI Acc No: 2002-750107/200281

XRPX Acc No: N02-590779

Security information updating method for remotely managed computer system, involves retrieving current password from security information stored in lockable memory device, accessible during power on self test

Patent Assignee: INT BUSINESS MACHINES CORP (IBM)

Inventor: CROMER D C; FREEMAN J W; GOODMAN S D; SPRINGFIELD R S; WARD J P

Number of Countries: 001 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020120845	A1	20020829	US 2001793239	A	20010226	200281 B
US 6823464	B2	20041123	US 2001793239	A	20010226	200477

Priority Applications (No Type Date): US 2001793239 A 20010226

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

US 20020120845	A1	7		H04L-009/00	
----------------	----	---	--	-------------	--

US 6823464	B2			G06F-001/24	
------------	----	--	--	-------------	--

Abstract (Basic): US 20020120845 A1

NOVELTY - The current password is retrieved from security information in memory device accessible only during power on self test (POST) and hard-locked prior to loading operating system. A hash is generated using the current password appended, responsive to detecting a change request within non-volatile buffer. The security information is updated according to the change request, when **hash** generated **matches** a **hash** within the buffer.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

- (1) Security information updating system; and
- (2) Security information updating program.

USE - For remotely managed data processing system.

ADVANTAGE - Enables authentication of a remote entity to **allow** **changes** by the remote entity to hard-locked security information without compromising security, closing the current void between remote manageability and security. Allows a secure client to be remotely managed.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the data processing system.

pp; 7 DwgNo 1/2

Title Terms: SECURE; INFORMATION; UPDATE; METHOD; REMOTE; COMPUTER; SYSTEM; RETRIEVAL; CURRENT; PASSWORD; SECURE; INFORMATION; STORAGE; LOCK; MEMORY; DEVICE; ACCESS; POWER; SELF; TEST

Derwent Class: T01; W01

International Patent Class (Main): G06F-001/24 ; H04L-009/00

File Segment: EPI

23/5/4 (Item 4 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2006 Thomson Derwent. All rts. reserv.

013725907 **Image available**

WPI Acc No: 2001-210137/200121

XRPX Acc No: N01-150063

User identity authentication for computer network, by sending template with biometric data to client and computing primary and secondary messages at host and client respectively, based on which authenticity is judged

Patent Assignee: ORACLE CORP (ORAC-N)

Inventor: GILCHRIST G; VIAVANT S D

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6167517	A	20001226	US 9858394	A	19980409	200121 B

Priority Applications (No Type Date): US 9858394 A 19980409

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6167517	A	12		H04L-009/08	

Abstract (Basic): US 6167517 A

NOVELTY - User identifier is received from clients (102,104,106) at host systems (108,110,112), and associated template with biometric data is retrieved. Client compares template with biometric sample. Primary message is computed using template, **comparison** result and an **encryption** key. Host computes secondary message using primary message received from client, based on which user is **allowed to access** the host system.

DETAILED DESCRIPTION - The secondary message digest is computed on the host system using template, comparison result indicating successful match between biometric sample and template, and encryption key. The templates are retrieved from database of templates by the host system. The template includes fingerprint data, retinal scan data, voice data or handwriting data. INDEPENDENT CLAIMS are also included for the following:

- (a) Apparatus for authenticating identity of user;
- (b) User authentication program

USE - Used for computer network.

ADVANTAGE - Using the template in computing the message, digest provides an additional measure of security, because the message digests do not match unless the client also used the template for computing message digest. This indicates that the client computed the comparison result using the same template. The use of randomized number in computing the message digest, prevents a simple mode of attack. Client using comparison threshold prevents malicious user on the client from setting the comparison threshold to an arbitrary low value in order to gain unauthorized access to the host system. Thus, the method achieves secured access of client to the host system.

DESCRIPTION OF DRAWING(S) - The figure shows the client computer system coupled to host system through network.

Clients (102,104,106)

Host systems (108,110,112)

pp; 12 DwgNo 1/4

Title Terms: USER; IDENTIFY; AUTHENTICITY; COMPUTER; NETWORK; SEND; TEMPLATE; DATA; CLIENT; COMPUTATION; PRIMARY; SECONDARY; MESSAGE; HOST; CLIENT; RESPECTIVE; BASED; AUTHENTICITY; JUDGEMENT

Derwent Class: S05; T01; T04; T05; W01; W04

International Patent Class (Main): H04L-009/08
File Segment: EPI

23/5/5 (Item 5 from file: 350)
DIALOG(R) File 350:Derwent WPIX
(c) 2006 Thomson Derwent. All rts. reserv.

012753581
WPI Acc No: 1999-559698/199947
XRPX Acc No: N99-413298

Restricting scheme of execution of unlicensed or virus-infected software on a hardware platform - includes using private key stored in embedded security coprocessor or code key obtained by coprocessor and comparing keys to determine if access is allowed

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
RD 425106	A	19990910	RD 99425106	A	19990820	199947 B

Priority Applications (No Type Date): RD 99425106 A 19990820

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
RD 425106	A		2	G06F-000/00	

Abstract (Basic): RD 425106 A

NOVELTY - An embedded security coprocessor can be used to sign an executable using a private key stored in the coprocessor and the signature is compared to an attached signature on the executable to determine if execution is to be allowed. The coprocessor can also be used to obtain a DES key, which is used to decrypt the executable before it is run or the header of the executable can be decrypted using a DES key obtained via the hardware security coprocessor. The executable would be hashed and the two **hashes compared**, to determine if execution will be allowed.

USE - Restricting execution of unlicensed or virus-infected software on a hardware platform.

Dwg.0/0

Title Terms: RESTRICT; SCHEME; EXECUTE; VIRUS; INFECT; SOFTWARE; HARDWARE; PLATFORM; PRIVATE; KEY; STORAGE; EMBED; SECURE; CODE; KEY; OBTAIN; COMPARE; KEY; DETERMINE; ACCESS; ALLOW

Derwent Class: T01

International Patent Class (Main): G06F-000/00

File Segment: EPI

23/5/6 (Item 6 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2006 Thomson Derwent. All rts. reserv.

011778881 **Image available**

WPI Acc No: 1998-195791/199818

XRXPX Acc No: N98-155051

ID code protection device for mobile radio telephone - stores ID number and encrypted ID number in memory and performs comparison with input number each time telephone is to be used to authorise or prevent access

Patent Assignee: PHILIPS ELECTRONICS NV (PHIG); PHILIPS GLOEILAMPENFAB NV (PHIG)

Inventor: RESTIF P

Number of Countries: 021 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 835007	A1	19980408	EP 97202313	A	19970724	199818	B
JP 10094058	A	19980410	JP 97203521	A	19970729	199825	
KR 98010987	A	19980430	KR 9737432	A	19970731	199916	
CN 1175830	A	19980311	CN 97116150	A	19970731	200209	

Priority Applications (No Type Date): FR 969640 A 19960731

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

EP 835007	A1	F	6	H04L-009/32	
-----------	----	---	---	-------------	--

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

JP 10094058	A	4	H04Q-007/38
-------------	---	---	-------------

KR 98010987	A		G09G-003/28
-------------	---	--	-------------

CN 1175830	A		H04K-001/02
------------	---	--	-------------

Abstract (Basic): EP 835007 A

The device has an ID number (ESN) which is stored in device memory (54). The ID number is encrypted using and this encrypted code is also stored in the memory. These codes are placed in memory during device manufacture.

Each time the device is used, an active protection **comparison** system (K10) **encrypts** an incoming number and compares it with the stored encrypted number. If the numbers agree, the mechanism is activated and the stored ID number is re-encrypted.

USE - AMPS, TAC or ETAC system.

ADVANTAGE - Provides improved protection against fraudulent use without utilising constructor code. Low cost.

Dwg.3/5

Title Terms: ID; CODE; PROTECT; DEVICE; MOBILE; RADIO; TELEPHONE; STORAGE; ID; NUMBER; ENCRYPTION; ID; NUMBER; MEMORY; PERFORMANCE; COMPARE; INPUT; NUMBER; TIME; TELEPHONE; AUTHORISE; PREVENT; ACCESS

Derwent Class: P85; W01

International Patent Class (Main): G09G-003/28; H04K-001/02; H04L-009/32 ; H04Q-007/38

International Patent Class (Additional): G09C-001/00

File Segment: EPI; EngPI

17/5/2 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2006 Thomson Derwent. All rts. reserv.

013362362 **Image available**

WPI Acc No: 2000-534301/200049

XRPX Acc No: N00-395259

Authorizing **film holder** to access **remote look-up table of film photo finishing** data, matching encrypted segments of access code

Patent Assignee: EASTMAN KODAK CO (EAST)

Inventor: CIPOLLA D; SMART D C

Number of Countries: 027 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 1016926	A2	20000705	EP 99204275	A	19991213	200049 B
JP 2000231162	A	20000822	JP 99365608	A	19991222	200055
US 6222993	B1	20010424	US 98221942	A	19981228	200125

Priority Applications (No Type Date): US 98221942 A 19981228

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

EP 1016926 A2 E 43 G03D-015/00

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
LI LT LU LV MC MK NL PT RO SE SI

JP 2000231162 A 36 G03B-027/46

US 6222993 B1 G03B-017/02

Abstract (Basic): EP 1016926 A2

NOVELTY - Film is registered by docking (138) in input device and reading first segment of identifier marked on film, which includes one or both segments of access code. One segment of access code is encryption of other segment. User or holder of film can only access data stored in look-up table (12) if code value obtained by decrypting first segment, matches second segment.

DETAILED DESCRIPTION - Film is registered by docking in input device and reading first segment of identifier marked on film. Identifier includes one or both segments of access code. One segment is encryption of other. User or holder of film can only access data stored in look-up table (12) if code value obtained by decrypting first segment, matches second segment. Key used to decrypt encrypted first segment of access code, is maintained and supplied by input or photo finishing unit (14), or by gatekeeper part of look-up table. Key is based on symmetric encryption-decryption algorithm or asymmetric encryption-decryption algorithm.

USE - To access film photo finishing data stored in remote look-up table for one-time use camera.

DESCRIPTION OF DRAWING(S) - View of system including access coded film unit.

Look-up table (12)

Photo finishing unit (14)

pp; 43 DwgNo 20/21

Title Terms: FILM; HOLD; ACCESS; REMOTE; UP; TABLE; FILM; PHOTO; FINISH; DATA; MATCH; ENCRYPTION; SEGMENT; ACCESS; CODE

Derwent Class: P82; P84; S06; T01

International Patent Class (Main): G03B-017/02; G03B-027/46; G03D-015/00

International Patent Class (Additional): G03B-017/24; G03B-017/48; G03B-027/72; G06F-017/30

File Segment: EPI; EngPI

17/5/4 (Item 4 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2006 Thomson Derwent. All rts. reserv.

011792732 **Image available**

WPI Acc No: 1998-209642/199819

XRPX Acc No: N98-166604

Financial services subscriber access method e.g. for remote banks, insurance companies - using unique identifiers for each customer and each card which are verified when card is used by comparison with stored ID data and encrypted data sent from card via communications network

Patent Assignee: FINTEL SA (FINT-N); FINTEL (FINT-N)

Inventor: GAYET A; MOULIN J; ROSSET F

Number of Countries: 080 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2753860	A1	19980327	FR 9611915	A	19960925	199819	B
WO 9813971	A1	19980402	WO 97FR1682	A	19970925	199820	
AU 9743888	A	19980417	AU 9743888	A	19970925	199834	
EP 950303	A1	19991020	EP 97942087	A	19970925	199948	
			WO 97FR1682	A	19970925		
JP 2001508563	W	20010626	WO 97FR1682	A	19970925	200140	
			JP 98515345	A	19970925		
US 6704715	B1	20040309	WO 97FR1682	A	19970925	200418	
			US 99269079	A	19990520		

Priority Applications (No Type Date): FR 9611915 A 19960925

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

FR 2753860 A1 12 H04L-009/32

WO 9813971 A1 F 27 H04L-009/32

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW

Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GH GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9743888 A H04L-009/32 Based on patent WO 9813971

EP 950303 A1 F H04L-009/32 Based on patent WO 9813971

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE SI

JP 2001508563 W 26 G06F-015/00 Based on patent WO 9813971

US 6704715 B1 G06F-017/60 Based on patent WO 9813971

Abstract (Basic): FR 2753860 A

The method involves the bank or insurance company providing each of their customers with a credit card type card (10) which contains unique identifiers for each card and for each customer. The card generates short acoustic encrypted ID signals of DTMF type when it is used.

The acoustic signals are received at a microphone and transmitted to the bank or insurance company via a communications network. The ID signals are processed and decrypted and compared with the ID data for the card and for the customer and access to services is permitted if they coincide.

ADVANTAGE - Allows subscribers rapid remote access to bank or insurance services while preventing fraudulent access or use of stolen card.

Dwg.1/1

Title Terms: FINANCIAL; SERVICE; SUBSCRIBER; ACCESS; METHOD; REMOTE; BANK; INSURANCE; COMPANY; UNIQUE; IDENTIFY; CUSTOMER; CARD; VERIFICATION; CARD; COMPARE; STORAGE; ID; DATA; ENCRYPTION; DATA; SEND; CARD; COMMUNICATE;

NETWORK

Derwent Class: P85; T01; T05; U23; W01

International Patent Class (Main): G06F-015/00; G06F-017/60

International Patent Class (Additional): G06F-019/00; G09C-001/00;
H04L-009/32; H04M-001/274; H04M-003/50

File Segment: EPI; EngPI

13/5/4 (Item 1 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2006 Thomson Derwent. All rts. reserv.

013652094 **Image available**

WPI Acc No: 2001-136306/200114

Related WPI Acc No: 2000-571006

XRPX Acc No: N01-099123

Compressed file name generating method in client-server system, involves comparing generated file names, based on which file command is executed with respect to file identified by particular file name

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)

Inventor: RIETH P F; STEVENS J S

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6134597	A	20001017	US 97864052	A	19970528	200114 B

Priority Applications (No Type Date): US 97864052 A 19970528

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

US 6134597	A	13	G06F-015/16
------------	---	----	-------------

Abstract (Basic): US 6134597 A

NOVELTY - The server is activated by a request from user and without reference to any prompting for user assigned credentials to build respective input strings with user profile from respective requests, user attitude and hidden key. File names are generated by concatenating tags generated by hashing input strings with fixed identifiers. The file names are compared based on which file command is executed.

DETAILED DESCRIPTION - User attribute and a hidden key value are stored at server. Initial request including file name, user profile and file data is communicated from user to server. The server is operated in response to initial request and without reference to any prompting for user assigned credentials. A first input string including the user profile is built from initial request, user attribute and hidden key value. The first input string is hashed to generate a first tag which is concatenated with fixed identifier to generate a first file name for file data. The first data identified by first file name is stored. A subsequent request including user profile, file name and file command is communicated to server from user. The server is operated at session initialization in the same manner to build a second input string. A **second file** name is generated by concatenating second tag generated by hashing second input string. The **second file** name is **compared** with **first file** name and if they are equal, the file command is executed with respect to **file** identified by **first file** name.

INDEPENDENT CLAIMS are also included for the following:

(a) server system;

(b) client **access authorizing** program

USE - In client-server system such as in TCP/IP or Internet environment.

ADVANTAGE - Provides a system for identifying objects with a user unique, compressed tag. Provides a user unique, compressed tag in a manner which is transparent to the user. Provides a user unique, compressed tag from publicly available information.

DESCRIPTION OF DRAWING(S) - The figure shows conceptual diagram illustrating several programming entities and objects of client-server system.

pp; 13 DwgNo 1/4

Title Terms: COMPRESS; FILE; NAME; GENERATE; METHOD; CLIENT; SERVE; SYSTEM;
COMPARE; GENERATE; FILE; NAME; BASED; FILE; COMMAND; EXECUTE; RESPECT;
FILE; IDENTIFY; FILE; NAME

Derwent Class: T01

International Patent Class (Main): G06F-015/16

File Segment: EPI

17/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2006 Thomson Derwent. All rts. reserv.

013167049 **Image available**
WPI Acc No: 2000-338922/200029
XRPX Acc No: N00-254446

User authentication for data accessing in computer system, involves comparing identity information received from user with identity information in authenticating computer to authenticate user to access required data

Patent Assignee: SYMANTEC CORP (SYMA-N)
Inventor: GRAWROCK D
Number of Countries: 021 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200019300	A1	20000406	WO 99US21924	A	19990921	200029 B
EP 1135719	A1	20010926	EP 99969806	A	19990921	200157
			WO 99US21924	A	19990921	
US 6360322	B1	20020319	US 98162102	A	19980928	200224

Priority Applications (No Type Date): US 98162102 A 19980928

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200019300	A1	E	32	G06F-001/00	
				Designated States (National):	CA
				Designated States (Regional):	AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
EP 1135719	A1	E		G06F-001/00	Based on patent WO 200019300
				Designated States (Regional):	AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
US 6360322	B1			G06F-001/26	

Abstract (Basic): WO 200019300 A1

NOVELTY - The user's computer remote from authenticating entity stores **encrypted data**. The authenticating computer at authenticating entity **compares** identity **information** received from user with a prestored identity information, so that if both information are correlated, user is authenticated to access desired data by automatically providing an access key.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for user authentication system.

USE - For authenticating data accessing by user in computer system.

ADVANTAGE - Allows user to gain **access** to computer data even if password is forgotten while maintaining the data security.

DESCRIPTION OF DRAWING(S) - The figure shows the security system.
pp; 32 DwgNo 2/6

Title Terms: USER; AUTHENTICITY; DATA; ACCESS; COMPUTER; SYSTEM; COMPARE; IDENTIFY; INFORMATION; RECEIVE; USER; IDENTIFY; INFORMATION; AUTHENTICITY ; COMPUTER; AUTHENTICITY; USER; ACCESS; REQUIRE; DATA

Derwent Class: T01

International Patent Class (Main): G06F-001/00; G06F-001/26

File Segment: EPI